NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 30, 2024

Michaelson Buchanan

Dear Sir:

Thank you for submitting a Standard Authorization Request (SAR) dated September 18, 2023 titled CIP-013-2 Supply Chain Risk Management with the purpose to revise CIP-012-3 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity, provide triggers on when the supply chain risk assessment(s) should be performed and require a response to risks identified.

Pursuant to Section 4.1 of the NERC Standard Processes Manual (SPM), Appendix 3A to the NERC Rules of Procedure, I am writing to inform you that on September 20, the Standards Committee (SC) reviewed the submitted SAR and voted to delay action pending consultation with the Reliability and Security Technical Committee (RSTC) to determine if there is another approach to addressing the issues laid out in the SAR.

For additional information on this matter, please see the attached background document and the SAR. These documents were considered at the September 20, 2023 SC meeting.

Sincerely,

Todd Bennett
Chair, NERC Standards Committee

cc:
Michaelson Buchanan, NERC Compliance
Holly Peterson, NERC Compliance
Rich Hydzik, Chair, RSTC
John Stephens, Vice Chair, RSTC
Stephen Crutchfield, Secretary, RSTC

Enclosures:
Standards Committee Background Document
CIP-013-2 Supply Chain Risk Management SAR

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

CIP-013-2 Supply Chain Risk Management

Action

- Accept the CIP-013-2 – Supply Chain Risk Management[1] Standard Authorization Request (SAR) submitted by the NERC critical infrastructure protection technical and compliance staff;
- Authorize posting of the SAR for a 30-day formal comment period; and
- Authorize solicitation of the SAR drafting team (DT) members.

Background

This project would address the current implementation of CIP-013, which has been wide-ranging and variable, potentially leading to incomplete or inaccurate supply chain risk evaluations. This project would revise CIP-013 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity. Additionally, it would provide triggers on when the supply chain risk assessment(s) must be performed (i.e., planning for procurement, procurement, and installation) and require a response to risks identified.

Summary

NERC staff recommends that the Standards Committee accept the CIP-013-2 SAR, authorize its posting for a 30-day formal comment period, and authorize the solicitation of DT members.

[1] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-2.pdf

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	CIP-013-2 Supply Chain Risk Management SAR		
Date Submitted:	September 18, 2023		
SAR Requester			
Name:	Michaelson Buchanan		
Organization:	NERC		
Telephone:	470.725.5268	Email:	michaelson.buchanan@nerc.net

SAR Type (Check as many as apply)

- ☐ New Standard
- ☒ Revision to Existing Standard
- ☐ Add, Modify, or Retire a Glossary Term
- ☐ Withdraw/retire an Existing Standard
- ☐ Imminent Action/ Confidential Issue (SPM Section 10)
- ☐ Variance development or revision
- ☐ Other (Please specify)

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)

- ☒ Regulatory Initiation
- ☐ Emerging Risk (Reliability Issues Steering Committee) Identified
- ☐ Reliability Standard Development Plan
- ☐ NERC Standing Committee Identified
- ☐ Enhanced Periodic Review Initiated
- ☐ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

The language in CIP-013-2 Requirement R1 lacks specificity to properly identify, assess, and respond to supply chain security risks. Specifically, Requirement R1 Part 1.1 does not indicate how to perform risk identification and assess vendor risks effectively. Additionally, CIP-013-2 does not contain sufficient triggers requiring activating an entity's supply chain risk management plan.

Industry implementation is wide ranging and variable across the ERO Enterprise. The implemented Industry supply chain risk processes are ambiguous and generally lack rigor for validating the completeness and accuracy of the data, assessing the risks, considering the vendor's mitigation activities, and documenting and tracking residual risks. This also leads to inconsistent information collected from vendors.

The lack of specificity for correctly identifying and assessing supply chain security risks may lead to incomplete or inaccurate risk evaluations. This may lead to supply chain risk likelihood and/or impact ratings that are not truly reflective of the actual risk posed to the entity.

Requested information
There is a lack of activation triggers to perform an entity's supply chain risk management program. The ambiguous language of Requirement R2's "Note" and the potential for a sizeable time delay between the actual procurement of equipment and the installation of the procured equipment. This delay could render the risk assessment outdated and potentially inaccurate during installation. An updated or revised risk assessment would ensure that all current and relevant risks are identified, assessed, and addressed. A requirement to update or re-perform a risk assessment for equipment or software before installation is necessary, as well as a time limit between the assessment and installation. There is a lack of tracking or responding to the risks identified through an entity's supply chain risk assessment. Requirement R1 Part 1.1 requires entities to "identify and assess," but the Standard does not require an entity to take any actions (i.e., respond) to any identified risks through the risk assessment. This includes accepting risks if they fall within a certain threshold. If accepted risks increase over time to a level above the entity's threshold, the entity may not be aware of the change due to the lack of tracking said risks. The majority, if not all, risk management frameworks hold fast to three pillars: 1. Identify, 2. Assess, and 3. Respond. Industry has many options to respond to risks, including mitigation, acceptance, transfer, and/or avoidance. Regardless of the option chosen, a response includes documenting and tracking the risk(s).
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
This project would revise CIP-013-2 to have complete and accurate assessments of supply chain security risks that reflect actual threat(s) posed to the entity. Additionally, it would provide triggers on when the supply chain risk assessment(s) must be performed (i.e., planning for procurement, procurement, and installation) and require a response to risks identified.
Project Scope (Define the parameters of the proposed project):
This project will make revisions to CIP-013-2 to require complete and accurate assessments of supply chain risks. Provide triggers of when activation of the supply chain risk assessment(s) must be performed and tracking and responding to all risks identified.
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide (1) a technical justification[1] that includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):
Revise CIP-013-2 to: • Require entities to create specific triggers to activate the supply chain risk assessment(s).

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

Requested information
• Include the performance of supply chain risk assessment(s) during the planning for procurement, procurement, installation of procured equipment/software/services, and post procurement assessment. • Include steps to validate the completeness and accuracy of the data, assess the risks, consider the vendor's mitigation activities, and document and track any residual risks. • Track and respond to all risks identified. • Re-assessment of standing contract risks on a set timeframe. • Re-assessment of time delay installation beyond a set timeframe.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
The Cost impact of implementing the proposed Standard depends on the method(s) by which a Responsible Entity chooses to meet any additional Requirements. However, a question will be asked during the comment period to ensure cost aspects are considered.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
No unique characteristics of BES facilities that may be impacted are known at this time.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g.*, Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide recommendations or findings from the consensus building activity.
SAR was developed in cooperation with and reviewed by voting members of the ERO CIP Compliance Task Force.
Are there any related standards or SARs that should be assessed for impact due to this proposed project? If so, which standard(s) or project number(s)?
None at this time.
Are there alternatives (e.g., guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the other options.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information
None at this time.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those that apply.	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operating of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for an emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained, and implemented.
☒	5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained qualified, and have the responsibility and authority to implement actions.
☒	7. The security of the interconnected bulk power systems shall be assessed, monitored, and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Market Interface Principles	
Does the proposed standard development project comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions from achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g., NPCC	None

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer